(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－344546
（P2001－344546A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	４１６	Ｇ０６Ｆ　17/60	４１６	
	２２２		２２２	
	４１４		４１４	
	５０２		５０２	
	５０６		５０６	

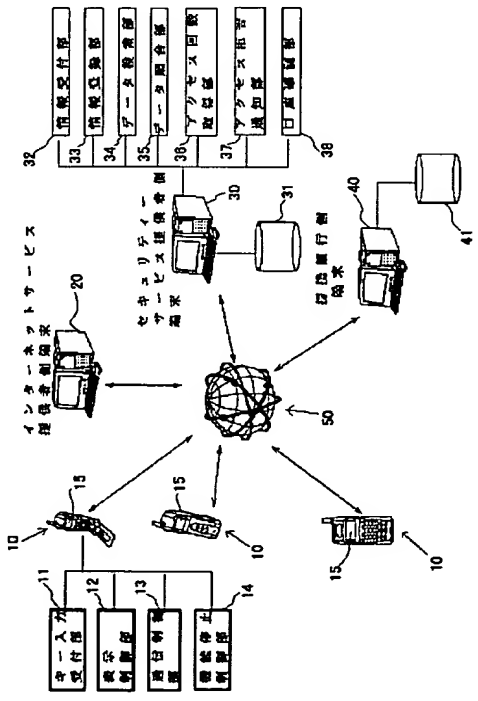
審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2001－96967(P2001－96967)
(22)出願日　平成13年３月29日(2001.3.29)
(31)優先権主張番号　特願2000－90291(P2000－90291)
(32)優先日　平成12年３月29日(2000.3.29)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　300018884
熊坂　憲二
東京都世田谷区八幡山３丁目33番１号　林マンション304
(72)発明者　熊坂　憲二
東京都世田谷区八幡山３丁目33番１号　林マンション304
(74)代理人　100097113
弁理士　堀　城之

(54)【発明の名称】　携帯情報端末の不正使用防止方法及び記録媒体

(57)【要約】
【課題】　携帯情報端末の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができるようにする。
【解決手段】　インターネットサービス提供者側端末２０がユーザーからの要求により情報提供サービスを行うとき、セキュリティーサービス提供者側端末３０がユーザーに関する利用者情報とパスワードとを加入者データベース３１から参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末４０がユーザーの銀行口座の残高を示す情報を口座情報データベース４１から参照してセキュリティサービス提供者側端末３０に与えるようにする。



1

【特許請求の範囲】

【請求項1】　ユーザーが携帯情報端末を用いて情報提供サービスを受ける第1の工程と、

インターネットサービス提供者側端末が前記携帯情報端末からの要求により前記情報提供サービスを行う第2の工程と、

前記インターネットサービス提供者側端末からの依頼により、セキュリティーサービス提供者側端末が前記ユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、前記インターネットサービス提供者側端末による前記情報提供サービスを許可する第3の工程と、

前記情報提供サービスが決済を伴うとき、セキュリティーサービス提供者側端末からの依頼により、提携銀行側端末が前記ユーザーの銀行口座の残高を示す情報を口座情報データベースから参照して前記セキュリティーサービス提供者側端末に与える第4の工程とを備えることを特徴とする携帯情報端末の不正使用防止方法。

【請求項2】　前記第1の工程には、

前記加入者データベースに登録するための利用者情報とパスワードとを送信する第5の工程と、

決済を伴う前記情報提供サービスを受けるとき、前記利用者情報とパスワードとを送信する第6の工程とが含まれ、

前記第2の工程には、前記利用者情報とパスワードとを受取ると、これらの情報を前記セキュリティーサービス提供者側端末に送信する第7の工程が含まれ、

前記第3の工程には、前記正規のユーザーであることが確認できたとき、直ちに前記銀行口座の残高を調べ、引き落としが可能かどうかを前記インターネットサービス提供者側端末を介して前記ユーザーに通知する第8の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項3】　前記第3の工程には、データ照合部により、前記加入者データベースから参照したデータが一致しないとき、正規のユーザーでないことを前記インターネットサービス提供者側端末に通知する第9の工程が含まれ、

前記第2の工程には、前記正規のユーザーでないことの通知を受けると、前記ユーザーのアクセスを拒否する第10の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項4】　前記第9の工程には、アクセス回数取得部により、前記ユーザーのアクセス拒否の回数と前記ユーザーの利用者情報とを保持し、一定回数以上のアクセス拒否が起きると、前記インターネットサービス提供者側端末に通知する第11の工程が含まれることを特徴とする請求項3に記載の携帯情報端末の不正使用防止方法。

【請求項5】　前記第1の工程には、正規のユーザーであることが確認された後、決済の意志を前記インターネットサービス提供者側端末に送信する第12の工程が含まれ、

前記第2の工程には、前記ユーザーからの決済の意志を前記セキュリティーサービス提供者側端末に送信する第13の工程が含まれ、

前記第3の工程には、口座確認部により、前記提携銀行側端末へ前記ユーザーの銀行口座からの代金の引き落としが可能かどうかを確認するための要求を行う第14の工程が含まれ、

前記第4の工程には、前記引き落としが可能かどうかを調べた結果を前記セキュリティーサービス提供者側端末に送信する第15の工程が含まれることを特徴とする請求項1に記載の携帯情報端末の不正使用防止方法。

【請求項6】　前記第12の工程には、前記引き落としが可能であるとき、決済の最終確認を前記インターネットサービス提供者側端末に通知する第16の工程が含まれ、

前記第13の工程には、前記セキュリティーサービス提供者側端末に引き落としの依頼を通知する第17の工程が含まれ、

前記第14の工程には、前記提携銀行側端末に引き落としの依頼を通知する第18の工程が含まれ、

前記第15の工程には、前記セキュリティーサービス提供者側端末に引き落としの完了を通知する第19の工程が含まれることを特徴とする請求項5に記載の携帯情報端末の不正使用防止方法。

【請求項7】　前記第18の工程には、前記インターネットサービス提供者側端末に引き落としの完了を通知する第20の工程が含まれ、

前記第17の工程には、前記携帯情報端末に引き落としの完了を通知する第21の工程が含まれることを特徴とする請求項6に記載の携帯情報端末の不正使用防止方法。

【請求項8】　前記利用者情報は、前記ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号であることを特徴とする請求項1、2又は4に記載の携帯情報端末の不正使用防止方法。

【請求項9】　前記利用者情報は、特定の文字列であることを特徴とする請求項1、2又は4に記載の携帯情報端末の不正使用防止方法。

【請求項10】　請求項1～9の何れかに記載の携帯情報端末の不正使用防止方法を実行可能なプログラムが記録されていることを特徴とする記録媒体。

【請求項11】　コンピュータに第1の工程～第4の工程を実行させるためのプログラム。

【請求項12】　コンピュータに第1の工程～第21の工程を実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話やノートパソコン等の携帯情報端末の使用者が正規の使用者であるか否かを特定して不正使用を防止したりオンラインショッピングなどの決済を行ったりする携帯情報端末の不正使用防止方法及び記録媒体に関する。

【0002】

【従来の技術】近年、携帯電話やノートパソコン等の携帯情報端末が普及している。これらは、使用する場所等が特定されないばかりか、たとえばインターネットを気軽に利用することができるようにもなっている。さらには、インターネットを用いてのオンラインショッピングの決済なども手軽に行われるようになっている。

【0003】

【発明が解決しようとする課題】ところで、上述した携帯電話やノートパソコン等の携帯情報端末の普及に伴い、紛失や盗難等の発生が増えている。これら携帯電話やノートパソコン等の携帯情報端末は、たとえば暗唱番号等を用いてのキーロック操作を行うことで、第3者の使用を防止できるようになっている。

【0004】ところが、使い勝手の面から暗唱番号等を用いてのキーロック操作を行う場合が少なく、たとえキーロック操作を行っても暗唱番号の解読等により、不正使用されてしまうことがある。このように、不正使用されると、たとえばオンラインショッピングの決済なども第3者によって行われることが予測され、正規の使用者が被害を被ることもあり得る。

【0005】このため、携帯電話やノートパソコン等の携帯情報端末の不正使用を確実に防止することができるシステムの開発が望まれている。

【0006】本発明は、このような状況に鑑みてなされたものであり、携帯情報端末の使用者が正規の使用者であるか否かを特定することで、不正使用を防止することができる携帯情報端末の不正使用防止方法及び記録媒体を提供することができるようにするものである。

【0007】

【課題を解決するための手段】請求項1に記載の携帯情報端末の不正使用防止方法は、ユーザーが携帯情報端末を用いて情報提供サービスを受ける第1の工程と、インターネットサービス提供者側端末が携帯情報端末からの要求により情報提供サービスを行う第2の工程と、インターネットサービス提供者側端末からの依頼により、セキュリティーサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、インターネットサービス提供者側端末による情報提供サービスを許可する第3の工程と、情報提供サービスが決済を伴うとき、セキュリティーサービス提供者側端末からの依頼により、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティーサービス提供者側端末に与える第4の工程とを備えることを特徴とする。また、第1の工程には、加入者データベースに登録するための利用者情報とパスワードとを送信する第5の工程と、決済を伴う情報提供サービスを受けるとき、利用者情報とパスワードとを送信する第6の工程とが含まれ、第2の工程には、利用者情報とパスワードとを受取ると、これらの情報をセキュリティーサービス提供者側端末に送信する第7の工程が含まれ、第3の工程には、正規のユーザーであることが確認できたとき、直ちに銀行口座の残高を調べ、引き落としが可能かどうかをインターネットサービス提供者側端末を介してユーザーに通知する第8の工程が含まれるようにすることができる。また、第3の工程には、データ照合部により、加入者データベースから参照したデータが一致しないとき、正規のユーザーでないことをインターネットサービス提供者側端末に通知する第9の工程が含まれ、第2の工程には、正規のユーザーでないことの通知を受けると、ユーザーのアクセスを拒否する第10の工程が含まれるようにすることができる。また、第9の工程には、アクセス回数取得部により、ユーザーのアクセス拒否の回数とユーザーの利用者情報とを保持し、一定回数以上のアクセス拒否が起きると、インターネットサービス提供者側端末に通知する第11の工程が含まれるようにすることができる。また、第1の工程には、正規のユーザーであることが確認された後、決済の意志をインターネットサービス提供者側端末に送信する第12の工程が含まれ、第2の工程には、ユーザーからの決済の意志をセキュリティーサービス提供者側端末に送信する第13の工程が含まれ、第3の工程には、口座確認部により、提携銀行側端末へユーザーの銀行口座からの代金の引き落としが可能かどうかを確認するための要求を行う第14の工程が含まれ、第4の工程には、引き落としが可能かどうかを調べた結果をセキュリティーサービス提供者側端末に送信する第15の工程が含まれるようにすることができる。また、第12の工程には、引き落としが可能であるとき、決済の最終確認をインターネットサービス提供者側端末に通知する第16の工程が含まれ、第13の工程には、セキュリティーサービス提供者側端末に引き落としの依頼を通知する第17の工程が含まれ、第14の工程には、提携銀行側端末に引き落としの依頼を通知する第18の工程が含まれ、第15の工程には、セキュリティーサービス提供者側端末に引き落としの完了を通知する第19の工程が含まれるようにすることができる。また、第18の工程には、インターネットサービス提供者側端末に引き落としの完了を通知する第20の工程が含まれ、第17の工程には、携帯情報端末に引き落としの完了を通知する第21の工程が含まれるようにすることができる。また、利用者情報は、ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号であるようにすることができる。また、利用者情報は、特定の文字列であるようにす

ることができる。請求項１０に記載の記録媒体は、請求項１～９の何れかに記載の携帯情報端末の不正使用防止方法を実行可能なプログラムが記録されていることを特徴とする。請求項１１に記載のプログラムは、コンピュータに第１の工程～第４の工程を実行させる。請求項１２に記載のプログラムは、コンピュータに第１の工程～第２１の工程を実行させる。本発明に係る携帯情報端末の不正使用防止方法及び記録媒体においては、インターネットサービス提供者側端末がユーザーからの要求により情報提供サービスを行うとき、セキュリティーサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティーサービス提供者側端末に与えるようにする。

【０００８】

【発明の実施の形態】以下、本発明の実施の形態について説明する。図１は、本発明の携帯情報端末の不正使用防止方法の一実施の形態に係る不正使用防止システムの概要を示す図、図２は、図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図、図３及び図４は、図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャート、図５～図１０は、図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【０００９】図１に示す不正使用防止システムは、一般ユーザーが使用する携帯情報端末１０、インターネットサービス提供者側端末２０、セキュリティーサービス提供者側端末３０及び提携銀行側端末４０を備え、これらはインターネット５０を介して相互に通信できるようになっている。

【００１０】携帯情報端末１０は、たとえば携帯電話、ノートパソコン、ＰＤＡ（個人情報端末）等の携帯型の通信手段である。携帯情報端末１０は、キー入力受付部１１、表示制御部１２、通信制御部１３、機能停止制御部１４を備えている。キー入力受付部１１は、携帯情報端末１０のキーからの入力を受付けるものである。

【００１１】表示制御部１２は、ディスプレイ１５への情報表示を制御するものである。通信制御部１３は、インターネット５０を介しての通信を制御するものである。機能停止制御部１４は、一定回数以上のアクセス拒否が起きると、セキュリティーサービス提供者側端末３０からの制御により、機能を停止させるものであり、その詳細は後述する。

【００１２】インターネットサービス提供者側端末２０は、オンラインショッピング等のサービスを提供するものである。セキュリティーサービス提供者側端末３０は、携帯情報端末１０の不正使用を防止したりするものであり、加入者データベース３１、情報受付部３２、情報登録部３３、データ検索部３４、データ照合部３５、アクセス回数取得部３６、アクセス拒否通知部３７、口座確認部３８を備えている。

【００１３】加入者データベース３１には、携帯情報端末１０の利用者情報とパスワードとが登録されるようになっている。ここで、利用者情報としては、一般ユーザーの氏名、住所、年齢、電話番号、顧客管理番号、銀行口座番号などである。また、これらの情報以外に、たとえばユーザーが指定した特定の文字列なども利用者情報として用いることができる。ここで、特定の文字列とは、たとえば好きな言葉であったり、詞であったり、歌詞であったり、何か意味をもつ内容であったりしてもよい。何れにしても、ユーザー個人のみが知り得るものであればよい。

【００１４】情報受付部３２は、携帯情報端末１０からの利用者情報やパスワードなどを受付けるものである。情報登録部３３は、受付けた利用者情報やパスワードなどを加入者データベース３１に登録するものである。

【００１５】データ検索部３４は、携帯情報端末１０からのアクセスに応じて加入者データベース３１に登録されているデータを検索するものである。データ照合部３５は、データ検索部３４によって検索されたデータの照合を行うものであり、データの照合が一致すると、正規のユーザーであると判断される。アクセス回数取得部３６は、データ照合部３５によるデータの照合の不一致に応じた携帯情報端末１０からのアクセス回数を取得するものである。

【００１６】アクセス拒否通知部３７は、アクセス回数取得部３６によるデータの照合の不一致のアクセスが一定回数以上であるとき、携帯情報端末１０側へ機能停止のための制御信号を送信する。このとき、携帯情報端末１０側では、機能停止制御部１４により、通信機能が停止される。また、携帯情報端末１０側の機能停止を行わせる場合、インターネットサービス提供者側端末２０へ機能停止のための制御信号を送信し、インターネットサービス提供者側端末２０からの通信キャリアの送信を停止させるようにすることもできる。口座確認部３８は、携帯情報端末１０からの決済の要求が生じたとき、提携銀行側端末４０の口座の残高を調べ、引き落としが可能かどうかを確認するものである。提携銀行側端末４０は、口座情報データベース４１を備えている。口座情報データベース４１は、ユーザーの銀行口座の残高などを管理するものである。

【００１７】次に、このような不正使用防止システムにおける携帯情報端末の不正使用防止方法の概要について説明する。

【００１８】まず、図２中の（１）は、ユーザーがたとえばオンラインショッピングなどの決済を必要とするサ

ービスを提供しているインターネットサイトにアクセスして、物品の購入などを行い決済の意志を伝えることを示す。このアクセスの際は、予め加入者データベース31に登録してある利用者情報とパスワードとを入力する。

【0019】これにより、利用者情報は一意であり、重複する番号はなく、パスワードは本人しか知り得ない情報であるため、アクセスしている人物が、正規のユーザーであるかどうかの判断ができる。

【0020】図2中の（2）は、インターネットサービス提供者が（1）で入力された利用者情報とパスワードとをセキュリティーサービス提供者に送信することを示す。図2中の（3）は、セキュリティーサービス提供者が（2）で受信したデータを使って、予め登録されている加入者データベース31を検索し、照合を行い、その結果を、インターネットサービス提供者に送信することを示す。

【0021】図2中の（4）は、インターネットサービス提供者が（3）で受信したデータを（1）でアクセスしてきたユーザーに送信することを示す。つまりここで、正規のユーザーであれば、予め登録してある氏名、住所、年齢、電話番号、銀行口座番号が表示されて確認をすることができる。正規のユーザーでなければ、アクセスが拒否された旨のメッセージが表示され、決済の処理が中止される。

【0022】このとき、セキュリティーサービス提供者では、アクセスが拒否された利用者情報とその回数を記録しておき、一定回数以上のアクセス拒否が起きると、その利用者情報を使用できなくするようにでき、安全性が高められる。同時に、登録されている氏名、住所宛てに郵送で利用者情報が使えなくなったことを伝えるようにすることができる。

【0023】図2中の（5）は、正規のユーザーであることが確認されたので再度、決済の意志をインターネットサービス提供者に送信することを示す。図2中の（6）は、インターネットサービス提供者がセキュリティーサービス提供者に（5）で受信したデータを送信することを示す。

【0024】図2中の（7）は、セキュリティーサービス提供者から、提携銀行へ（4）で認証されたユーザーの予め登録されている銀行口座から代金の引き落としが可能かどうかを確認することを示す。図2中の（8）は、提携銀行からセキュリティーサービス提供者へ引き落としが可能かどうかを調べた結果を送信することを示す。

【0025】図2中の（9）は、セキュリティーサービス提供者からインターネットサービス提供者へ（8）の情報を送信することを示す。図2中の（10）は、インターネットサービス提供者からユーザーへ（8）の結果を送信することを示す。つまりここで、引き落としが可能であれば次のステップへ進むことができる。引き落としが不可能であれば、その旨のメッセージが表示され、決済の処理が中止される。

【0026】図2中の（11）は、引き落としが可能であるため、決済の最終確認を行い、ユーザーの決済の意志をインターネットサービス提供者に送信することを示す。図2中の（12）は、インターネットサービス提供者がセキュリティーサービス提供者に引き落としの依頼を送信することを示す。

【0027】図2中の（13）は、セキュリティーサービス提供者が提携銀行に引き落としの依頼を送信することを示す。図2中の（14）は、提携銀行がセキュリティーサービス提供者に引き落としの完了を送信することを示す。図2中の（15）は、セキュリティーサービス提供者がインターネットサービス提供者に引き落としの完了を送信することを示す。図2中の（16）は、インターネットサービス提供者がユーザーに引き落としの完了を送信することを示す。

【0028】なお、全ての処理において、インターネット50上を通る情報は暗号化しておくと、さらに安全性が高められる。図2中の（2）の処理の後、セキュリティーサービス提供者では、正規のユーザーであることが確認できたら、直後に提携銀行の口座の残高を調べ、引き落としが可能かどうかを確認しておき、図2中の（9）の処理に戻るようにすることもできる。また、引き落としまで完了した場合、図2中の（15）の処理に戻るようにすることもできる。

【0029】次に、このような不正使用防止システムにおける携帯情報端末の不正使用防止方法について説明する。

【0030】まず、携帯情報端末10のユーザーは、予め自分の情報をセキュリティーサービス提供者30の加入者データベース31に登録しておく。加入者データベース31に登録される情報は、上述したユーザーの氏名、住所、年齢、電話番号、顧客管理番号、パスワード、銀行口座番号などである。また、上述したように、たとえばユーザーが指定した特定の文字列なども登録しておくことができる。

【0031】そして、まず、図3に示すように、ユーザーがたとえばオンラインショッピングなどの決済を必要とするサービスを提供しているインターネットサイトにアクセスする（ステップ201：図2中の（1））。ここで、物品の購入などを行い決済の意志を伝えるためのアクセスの際は、予め加入者データベース31に登録してある利用者情報とパスワードとを入力する。

【0032】このとき、携帯情報端末10のディスプレイ15には、たとえば図5に示すような内容が表示される。ここでは、利用者情報とパスワードの入力が促される。ここで、利用者情報とパスワードとを入力して『次へ』を操作すると、それらの情報がインターネットサー

ビス提供者側端末２０に送信される。

【００３３】これら利用者情報とパスワードとの入力が済むと（ステップ２０２）、インターネットサービス提供者側２０が図２中の（１）で入力された利用者情報とパスワードとをセキュリティーサービス提供者側端末３０に送信する（ステップ２０３：図２中の（２））。

【００３４】利用者情報とパスワードとを受けたセキュリティーサービス提供者側端末３０のデータ検索部３４により、図２中の（２）で受信したデータを使って、予め登録されている加入者データベース３１が検索されると、データ照合部３５により照合が行われ、照合が一致するとその結果が、インターネットサービス提供者側端末２０に送信される（ステップ２０４：図２中の（３））。

【００３５】その結果を受けたインターネットサービス提供者側端末２０は、図２中の（３）で受信したデータを図２中の（１）でアクセスしてきたユーザーに送信する（ステップ２０５：図２中の（４））。つまりここで、正規のユーザーであれば（ステップ２０６）、予め登録してある氏名、住所、年齢、電話番号、銀行口座番号や特定の文字列が表示されて確認をすることができる。これに対し、データ照合部３５により照合が不一致である場合、正規のユーザーでないため、アクセスが拒否された旨のメッセージが携帯情報端末１０のディスプレイ１５に表示され（ステップ２０７）、決済の処理が中止される。

【００３６】このとき、正規のユーザーであると確認されると、携帯情報端末１０の画面には、たとえば図６に示すような内容が表示され、その画面で『次へ』を操作すると、次のステップへ進むことができる。また、正規のユーザーでない場合、携帯情報端末１０の画面には、たとえば図７に示すような内容が表示される。

【００３７】このとき、セキュリティーサービス提供者側端末３０のアクセス回数取得部３６により、アクセスが拒否された利用者情報とその回数が保持され、一定回数以上のアクセス拒否が起きると、アクセス拒否通知部３７により、携帯情報端末１０側へ機能停止のための制御信号が送信される。このとき、携帯情報端末１０側では、機能停止制御部１４により、通信機能が停止される。また、携帯情報端末１０側の機能停止を行わせる場合、インターネットサービス提供者側端末２０へ機能停止のための制御信号を送信し、インターネットサービス提供者側端末２０からの通信キャリアの送信を停止させるようにすることもできる。

【００３８】これにより、携帯情報端末１０の使用が不可能となるため、安全性が高められる。同時に、登録されている氏名、住所宛てに郵送で利用者情報が使えなくなったことを伝えるようにすることができる。

【００３９】次いで、ユーザーは、正規のユーザーであることが確認されたので再度、決済の意志をインターネットサービス提供者側端末２０に送信する（ステップ２０８：図２中の（５））。決済の意志を受けたインターネットサービス提供者側端末２０は、セキュリティーサービス提供者側端末３０に図２中の（５）で受信したデータを送信する（ステップ２０９：図２中の（６））。

【００４０】そのデータを受信したセキュリティーサービス提供者側端末３０は、提携銀行側端末４０へ図２中の（４）で認証されたユーザーの予め登録されている銀行口座から代金の引き落としが可能かどうかを確認する（ステップ２１０：図２中の（７））。提携銀行側端末４０は、セキュリティーサービス提供者側端末３０へ引き落としが可能かどうかを調べた結果を送信する（ステップ２１１：図２中の（８））。

【００４１】引き落としが可能かどうかの結果を受けたセキュリティーサービス提供者側端末３０は、インターネットサービス提供者側端末２０へ図２中の（８）の情報を送信する（ステップ２１２：図２中の（９））。インターネットサービス提供者側端末２０は、ユーザーへ図２中の（８）の結果を送信する（ステップ２１３：図２中の（１０））。

【００４２】つまりここで、引き落としが可能であれば次のステップへ進むことができる。引き落としが不可能であれば、その旨のメッセージが表示され、決済の処理が中止される（ステップ２１４，２１５）。

【００４３】このとき、引き落としが可能であれば、携帯情報端末１０のディスプレイ１５には、たとえば図８に示すような内容が表示され、その画面で『次へ』を操作すると、次のステップへ進むことができる。また、引き落としが不可能であれば、携帯情報端末１０のディスプレイ１５には、たとえば図９に示すような内容が表示される。

【００４４】次に、図４に示すように、引き落としが可能であると、決済の最終確認を行うために、ユーザーの決済の意志をインターネットサービス提供者側端末２０に送信する（ステップ３０１：図２中の（１１））。インターネットサービス提供者側端末２０は、セキュリティーサービス提供者側端末３０に引き落としの依頼を送信する（ステップ３０２：図２中の（１２））。セキュリティーサービス提供者３０の口座確認部３８は、提携銀行４０に引き落としの依頼を送信する（ステップ３０３：図２中の（１３））。提携銀行側端末４０は、セキュリティーサービス提供者側端末３０に引き落としの完了を送信する（ステップ３０４：図２中の（１４））。

【００４５】セキュリティーサービス提供者側端末３０は、インターネットサービス提供者側端末２０に引き落としの完了を送信する（ステップ３０５：図２中の（１５））。インターネットサービス提供者側端末２０は、ユーザーに引き落としの完了を送信する（ステップ３０６：図２中の（１６））。このとき、携帯情報端末１０のディスプレイ１５には、たとえば図１０に示すような

内容が表示される。

【００４６】このように、本実施の形態では、インターネットサービス提供者側端末２０がユーザーからの要求により情報提供サービスを行うとき、セキュリティーサービス提供者側端末３０がユーザーに関する利用者情報とパスワードとを加入者データベース３１から参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末４０がユーザーの銀行口座の残高を示す情報を口座情報データベース４１から参照してセキュリティーサービス提供者側端末３０に与えるようにしたので、携帯情報端末１０の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができる。

【００４７】なお、本実施の形態では、オンラインショッピングの決済の場面などにおいて、本人であるかどうかを確認する場合について説明したが、この例に限らず、電話をかける直前、電話の電源を入れた直後なども同様に本人であるかどうかを確認するようにすることができる。

【００４８】さらに、セキュリティーサービス提供者側端末３０は、正規の登録者の情報でない照会が頻繁に起こった場合、通信キャリアを通じて、携帯情報端末１０の登録名義人に対して警告（お知らせ）を行うことができる。同時に通信キャリアでは、その携帯情報端末１０の使用を停止することもできる。

【００４９】なお、全ての処理において、インターネット５０上を通る情報は暗号化しておくと、さらに安全性が高められる。また、図２中の（２）の処理の後、セキュリティーサービス提供者側端末３０では、正規のユーザーであることが確認できたら、直後に提携銀行側端末４０の口座の残高を調べ、引き落としが可能かどうかを確認しておき、図２中の（９）の処理に戻るようにすることもできる。また、引き落としまで完了した場合、図２中の（１５）の処理に戻るようにすることもできる。

【００５０】

【発明の効果】以上の如く本発明に係る携帯情報端末の不正使用防止方法及び記録媒体によれば、インターネットサービス提供者側端末がユーザーからの要求により情報提供サービスを行うとき、セキュリティーサービス提供者側端末がユーザーに関する利用者情報とパスワードとを加入者データベースから参照し、正規のユーザーであると確認された場合に限り、情報提供サービスを許可するとともに、情報提供サービスが決済を伴うとき、提携銀行側端末がユーザーの銀行口座の残高を示す情報を口座情報データベースから参照してセキュリティーサービス提供者側端末に与えるようにしたので、携帯情報端末の使用者が正規の使用者であるか否かを特定することができ、不正使用を防止することができる。

【図面の簡単な説明】

【図１】本発明の携帯情報端末の不正使用防止方法の一実施の形態に係る不正使用防止システムの概要を示す図である。

【図２】図１の不正使用防止システムの概要を示す図である。

【図３】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャートである。

【図４】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するためのフローチャートである。

【図５】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図６】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図７】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図８】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

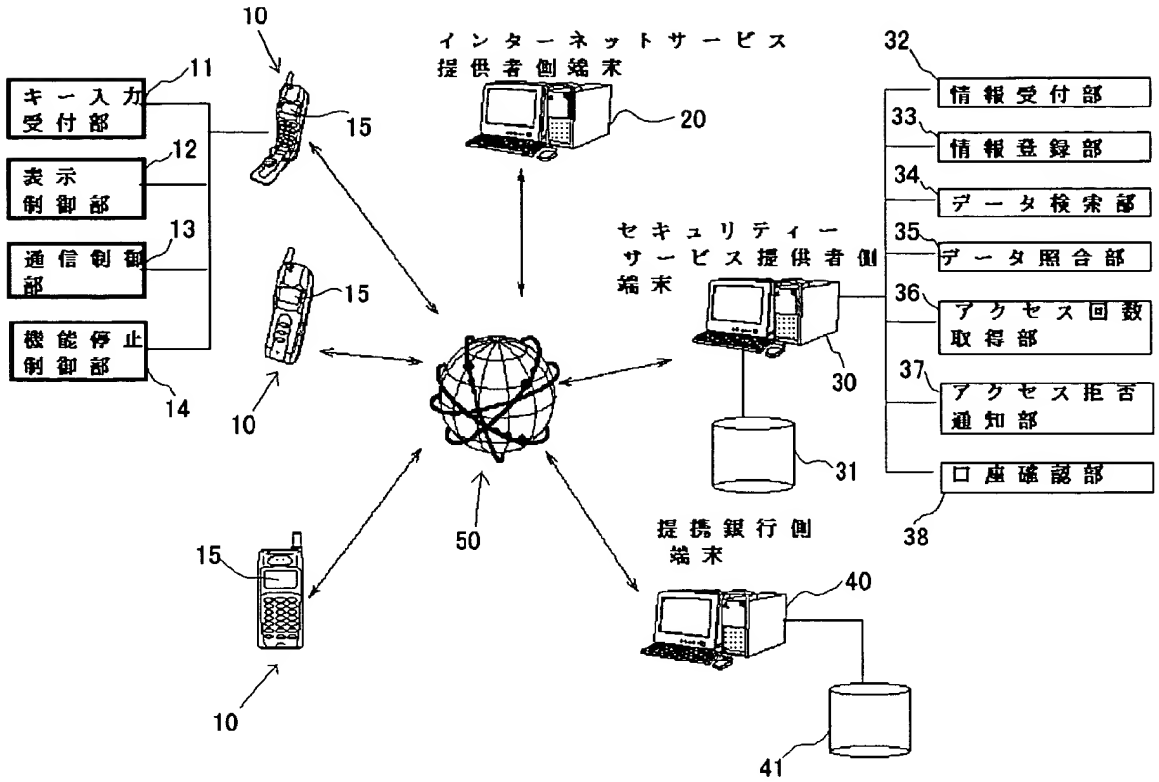
【図９】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

【図１０】図１の不正使用防止システムにおける携帯情報端末の不正使用防止方法を説明するための図である。

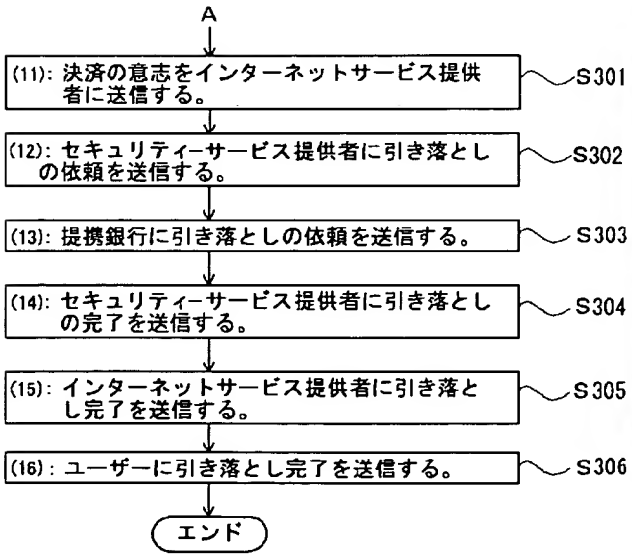
【符号の説明】

１０　携帯情報端末
２０　インターネットサービス提供者側端末
１１　キー入力受付部
１２　表示制御部
１３　通信制御部
１４　機能停止制御部
１５　ディスプレイ
３０　セキュリティーサービス提供者側端末
３１　加入者データベース
３２　情報受付部
３３　情報登録部
３４　データ検索部
３５　データ照合部
３６　アクセス回数取得部
３７　アクセス拒否通知部
３８　口座確認部
４０　提携銀行側端末
４１　口座情報データベース
５０　インターネット

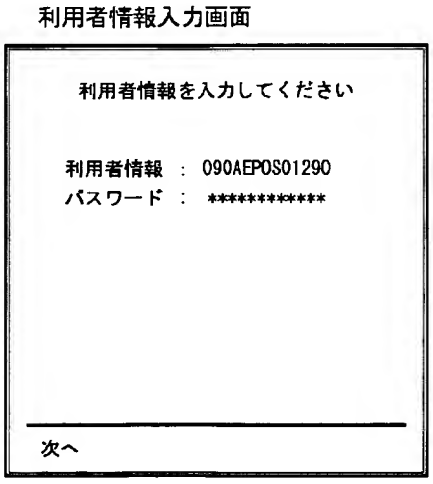
【図1】


10
11
キー入力受付部
12
表示制御部
13
通信制御部
機能停止制御部
14
15
インターネットサービス提供者側端末
20
32
情報受付部
33
情報登録部
34
データ検索部
35
データ照合部
36
アクセス回数取得部
37
アクセス拒否通知部
口座確認部
38
セキュリティーサービス提供者側端末
30
31
50
提携銀行側端末
40
41

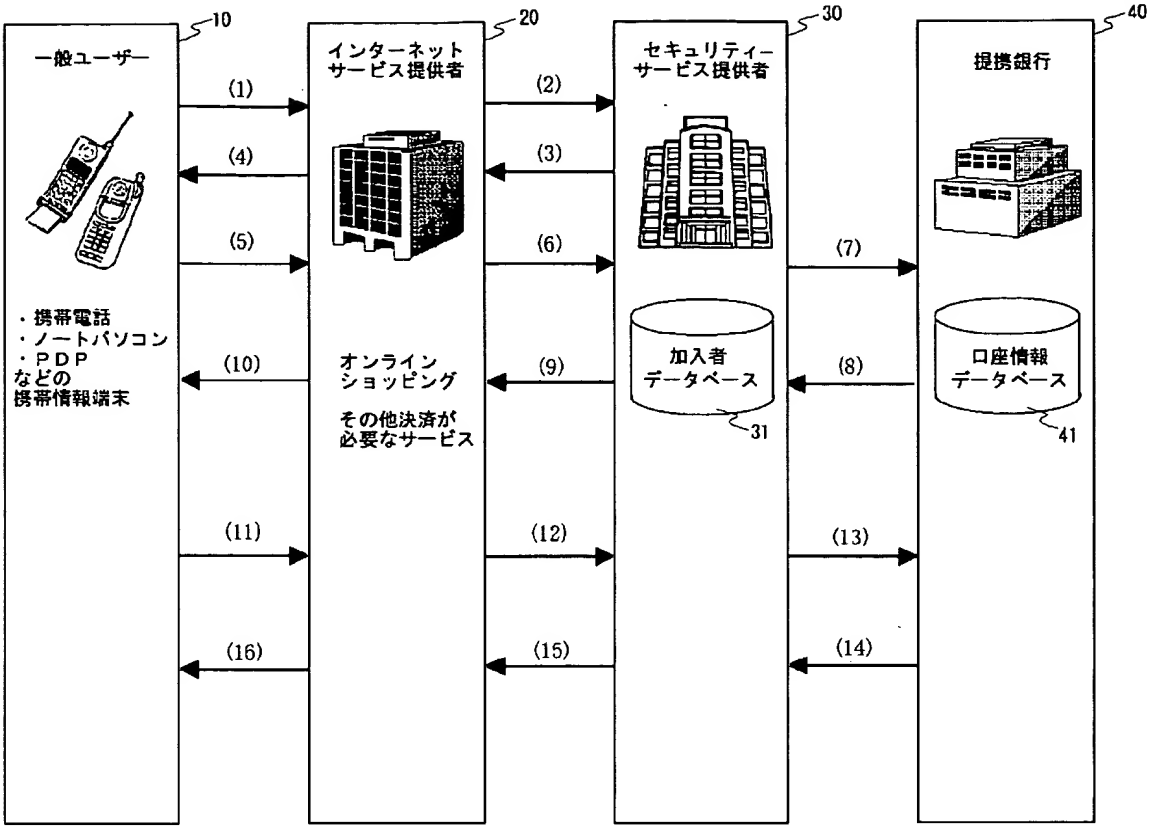
【図4】


A
(11): 決済の意志をインターネットサービス提供者に送信する。
S301
(12): セキュリティーサービス提供者に引き落としの依頼を送信する。
S302
(13): 提携銀行に引き落としの依頼を送信する。
S303
(14): セキュリティーサービス提供者に引き落としの完了を送信する。
S304
(15): インターネットサービス提供者に引き落とし完了を送信する。
S305
(16): ユーザーに引き落とし完了を送信する。
S306
エンド

【図5】


利用者情報入力画面
利用者情報を入力してください
利用者情報 : 090AEPOS01290
パスワード : **********
次へ

【図２】



【図６】

照会成功画面

照会成功

入力された利用者情報は承認されました。

次へ

【図７】

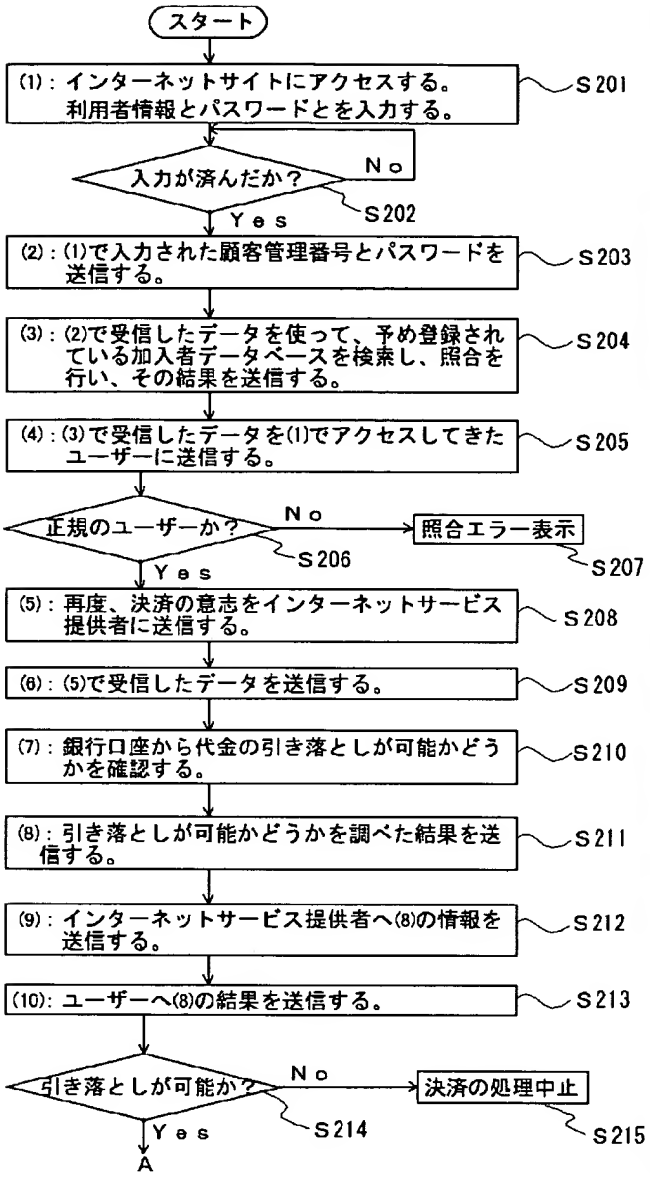
照会エラー画面

照会エラー

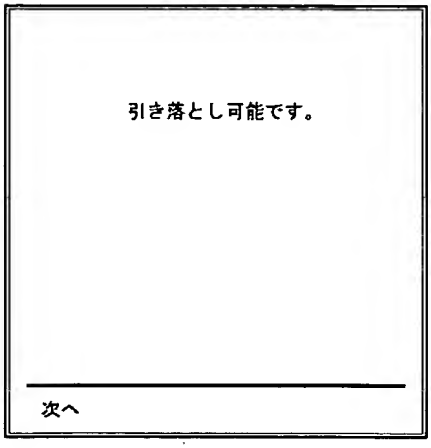
利用者情報が正しくありません。

確認

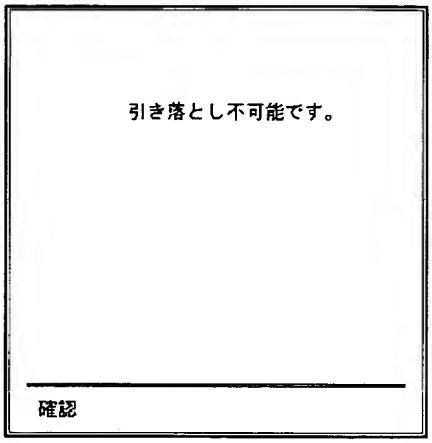
【図３】


スタート
(1)：インターネットサイトにアクセスする。利用者情報とパスワードとを入力する。
S201
入力が済んだか？
No
Yes
S202
(2)：(1)で入力された顧客管理番号とパスワードを送信する。
S203
(3)：(2)で受信したデータを使って、予め登録されている加入者データベースを検索し、照合を行い、その結果を送信する。
S204
(4)：(3)で受信したデータを(1)でアクセスしてきたユーザーに送信する。
S205
正規のユーザーか？
No
照合エラー表示
S207
Yes
S206
(5)：再度、決済の意志をインターネットサービス提供者に送信する。
S208
(6)：(5)で受信したデータを送信する。
S209
(7)：銀行口座から代金の引き落としが可能かどうかを確認する。
S210
(8)：引き落としが可能かどうかを調べた結果を送信する。
S211
(9)：インターネットサービス提供者へ(8)の情報を送信する。
S212
(10)：ユーザーへ(8)の結果を送信する。
S213
引き落としが可能か？
No
決済の処理中止
S215
Yes
S214
A

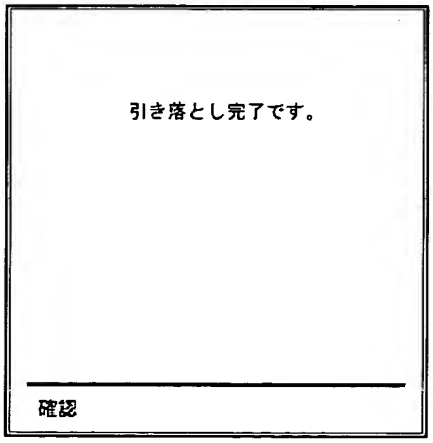
【図８】


引き落とし可能です。
次へ

【図９】


引き落とし不可能です。
確認

【図１０】


引き落とし完了です。
確認

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	